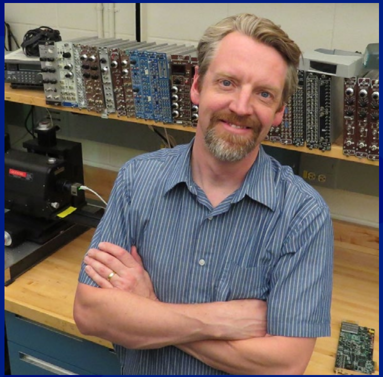
LA-UR-21-24923

Approved for public release; distribution is unlimited.

Title:	Frontiers in Science: Protecting the power grid with physics
Author(s):	Newell, Raymond Thorson
Intended for:	Online program
Issued:	2021-05-20

Frontiers In Science:

Protecting the power grid with physics



Raymond Newell

May 26, 2021 • 6pm

Power Grid Changes

- Grid upgrade for renewables, EV, etc.
- Communication & control: essential for future
- Must not introduce new vulnerability
- Need: secure communication

Los Alamos NATIONAL LABORATORY

The challenge: Current encryption systems rely on *computational difficulty*, often factoring a large number

**WWII:
The Enigma Machine**

Maybe it's not as hard as we think. . .

intel inside CORE i7

Progress of Computers

. . .the encrypted message could be stored and cracked years later

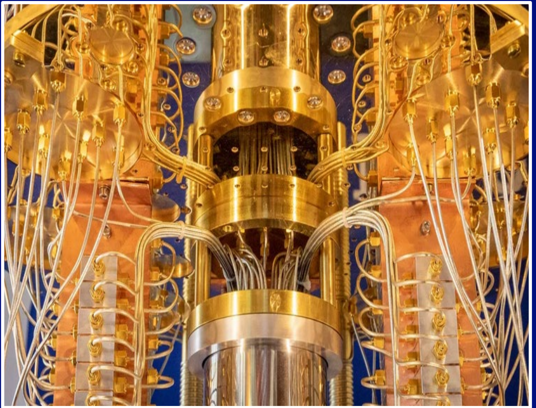


Image courtesy of IBM

53-qubit Quantum Computer Model

. . .and a quantum computer could do it easily!

The solution: Information is physical

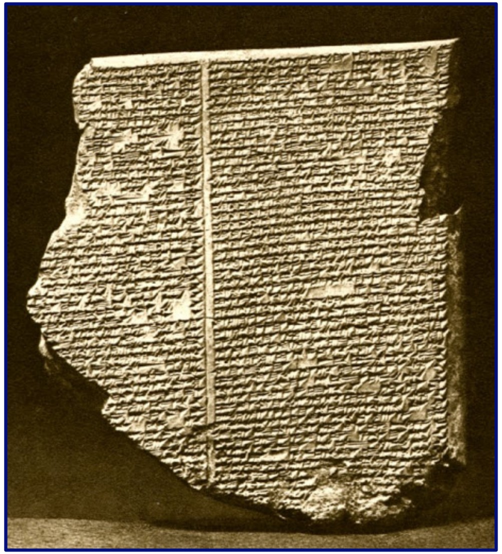
Quantum systems are well-suited for secret communication. Security is based on *fundamental laws of physics* rather than assumptions about adversary's abilities.

Classical information can be
- duplicated
- divided
- re-read

indefinitely, without alteration

Quantum information cannot be
- duplicated (no-cloning theorem)
- divided (no half-photons)
- re-read (wavefunction collapse)

Epic of Gilgamesh, ca. 1800 b.c.e.



A dream, ca. middle of the night

Quantum mechanics for secure communication

The BB-84 Protocol

- Encode information onto the state of a quantum system
- Send quantum system
- Measure system's state
  - Quantum system – single photons
  - State – their polarization

How do you build a system which obeys quantum laws, not classical ones?

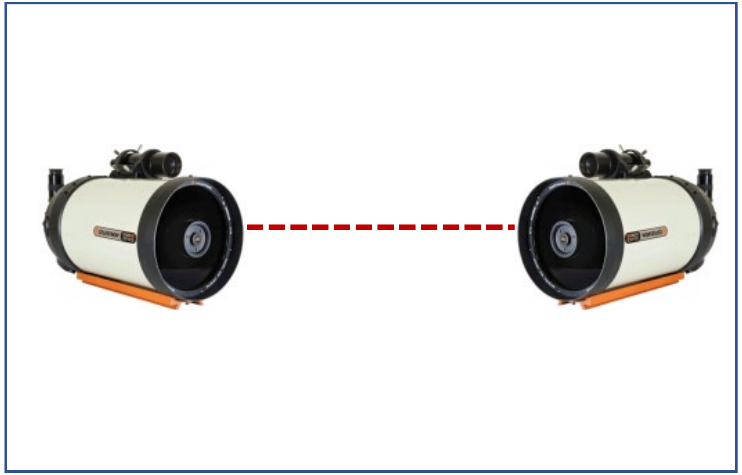
Get small!

Gilles Brassard

Charles H. Bennett

An optical technology…

Quantum communication requires an *optical* connection between terminals



Free Space

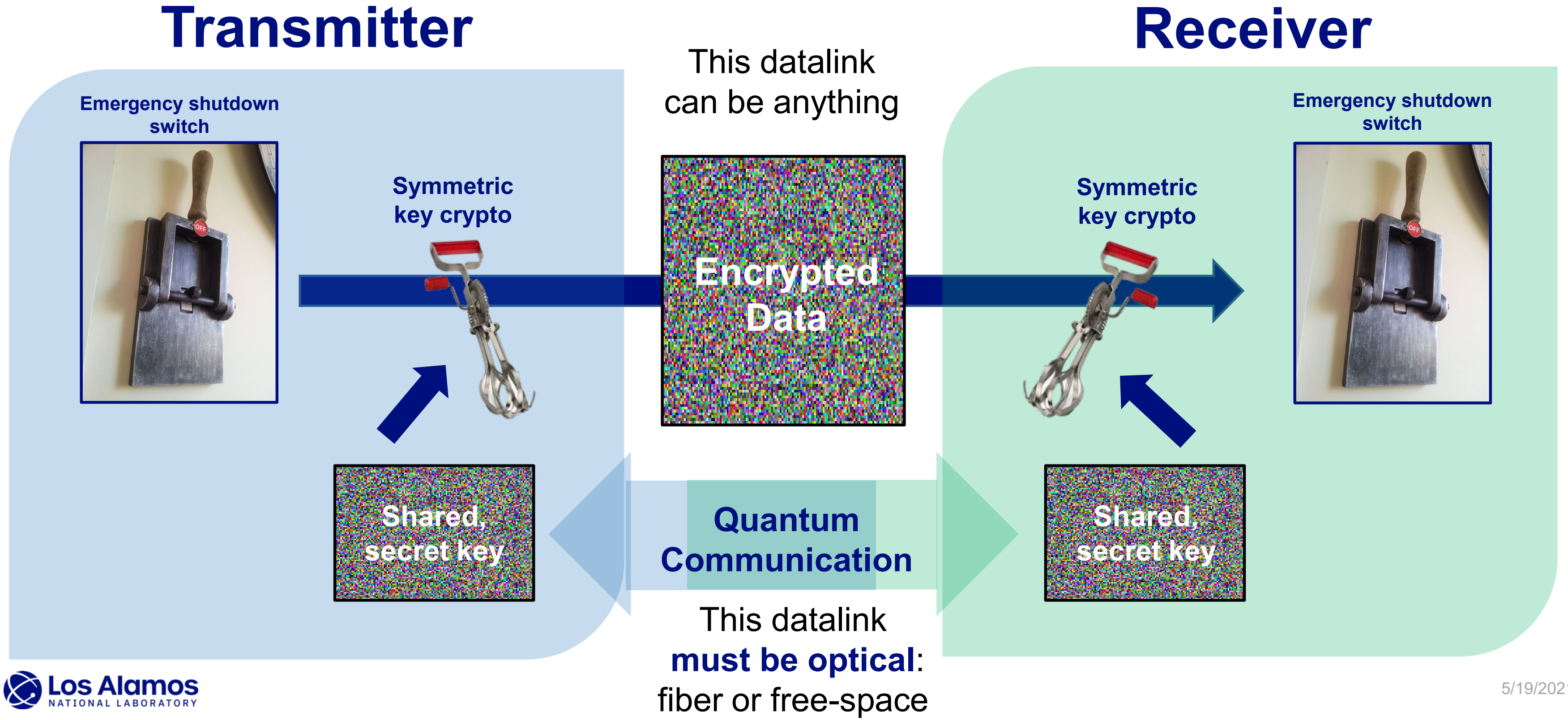
- Rooftop to rooftop
- Airplane to ground
- Ship to shore
- Satellite to ground

Fiber Optics

- Standard optical fibers
- Coexist with telecom data
- Within a building
- Metro area
- Up to 200 km

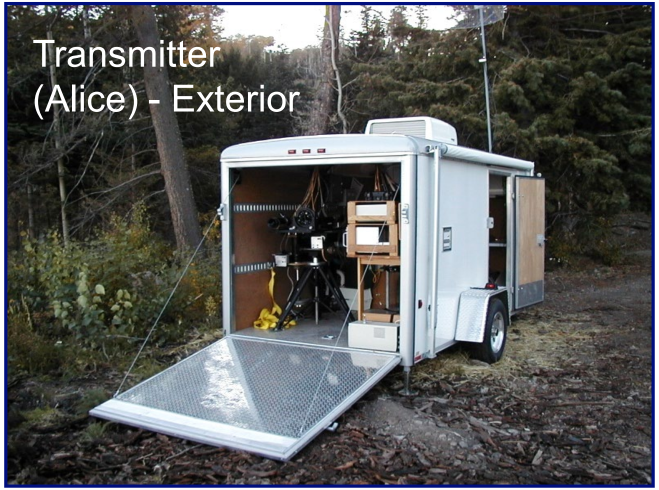
…use is not restricted to optics

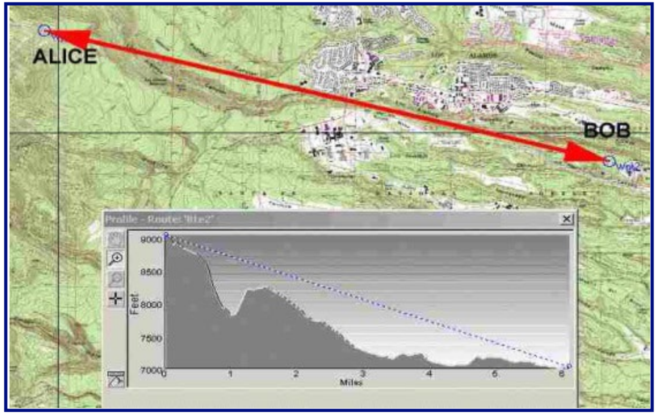
Once keys are generated, encryption can be used over *any* data link

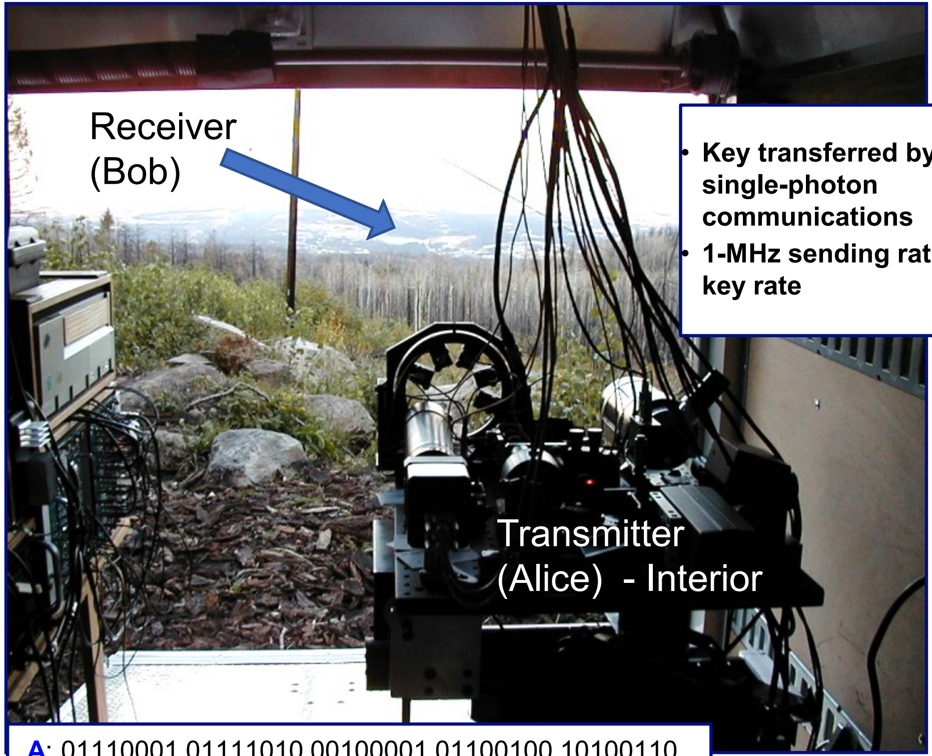


Example system: 10-km through the air link (1999)

10-km range in daylight one airmass path: comparable atmosphere to satellite-to-ground







- **Key transferred by 772-nm single-photon communications**
- **1-MHz sending rate; ~600-Hz key rate**

A: 01110001 01111010 00100001 01100100 10100110
B: 01110001 01111010 00100001 01100100 10100110

A: 11100010 00111101 10011111 10000111 11001111
B: 11100010 00111101 10011111 10000111 11001111

Example system: 1200-km through the air link (2017)

Science
AAAS

QUANTUM OPTICS

Satellite-based entanglement distribution over 1200 kilometers

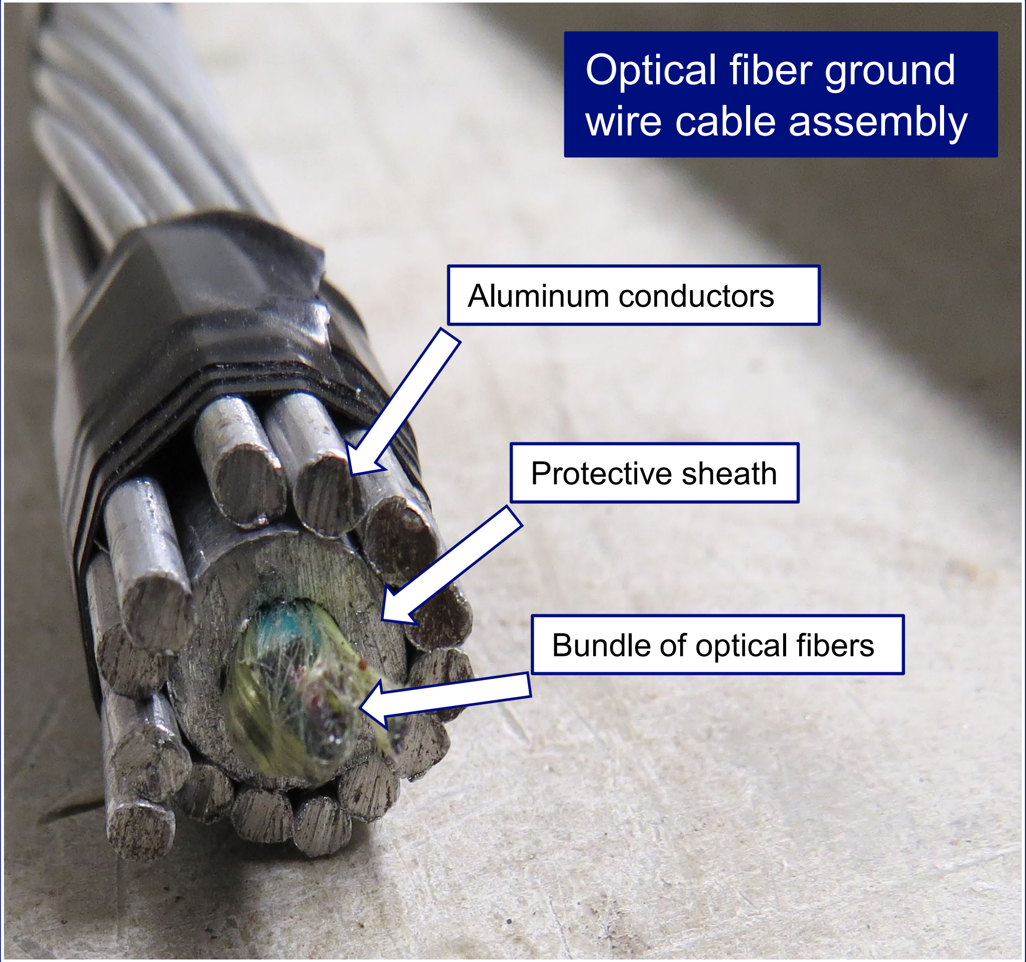
LETTER

nature
THE INTERNATIONAL WEEKLY JOURNAL OF SCIENCE

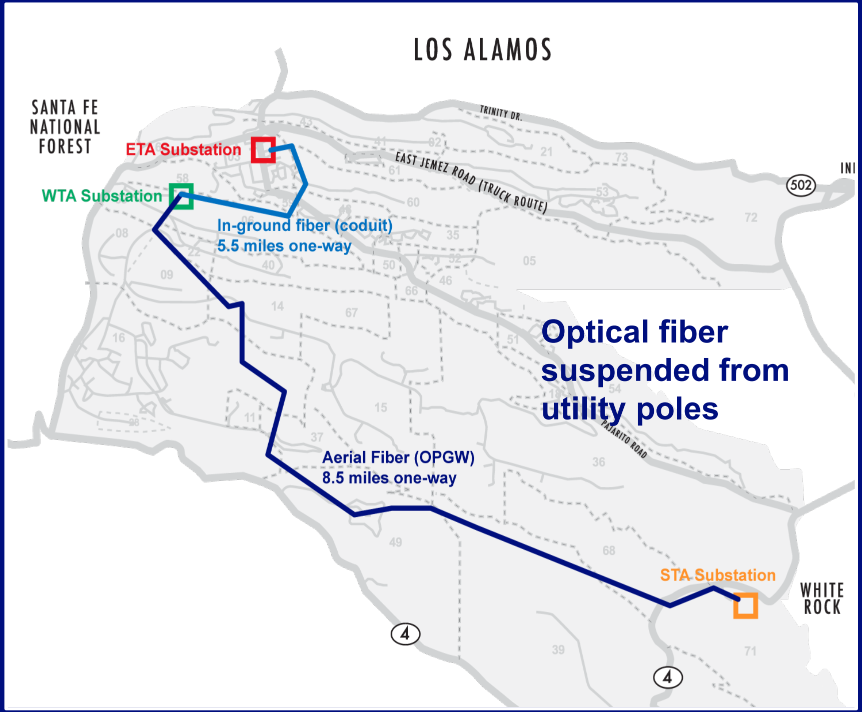
Ground-to-satellite quantum teleportation

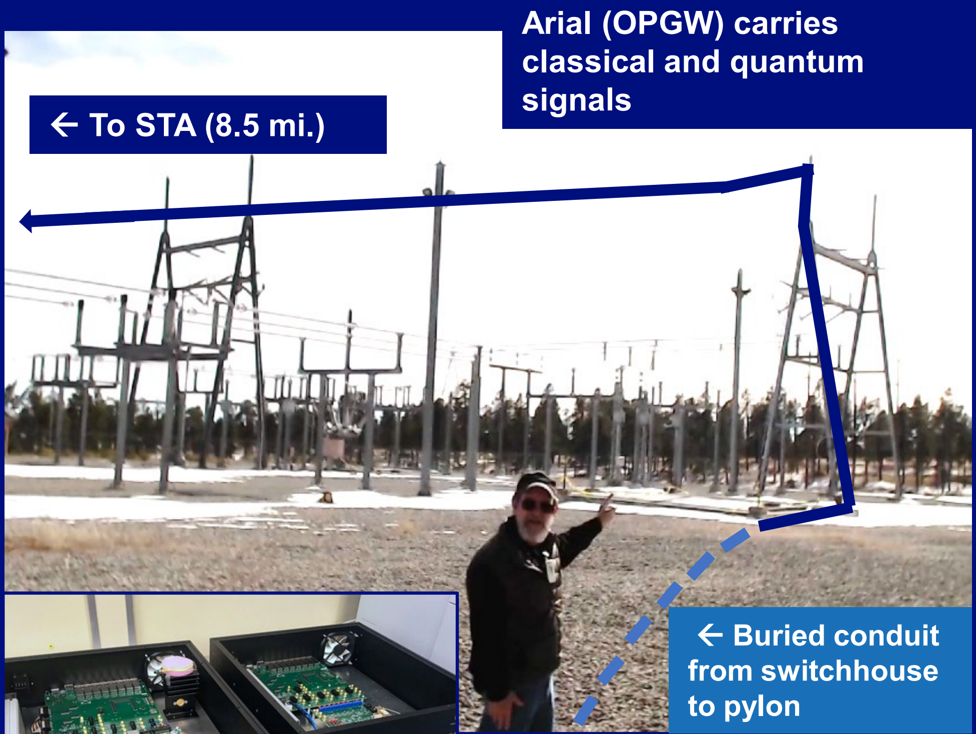
Quantum communication can be used as a bump-in-the-wire retrofit on existing control systems and networks

Invisible to end user,
but with much stronger security
– now and in the future

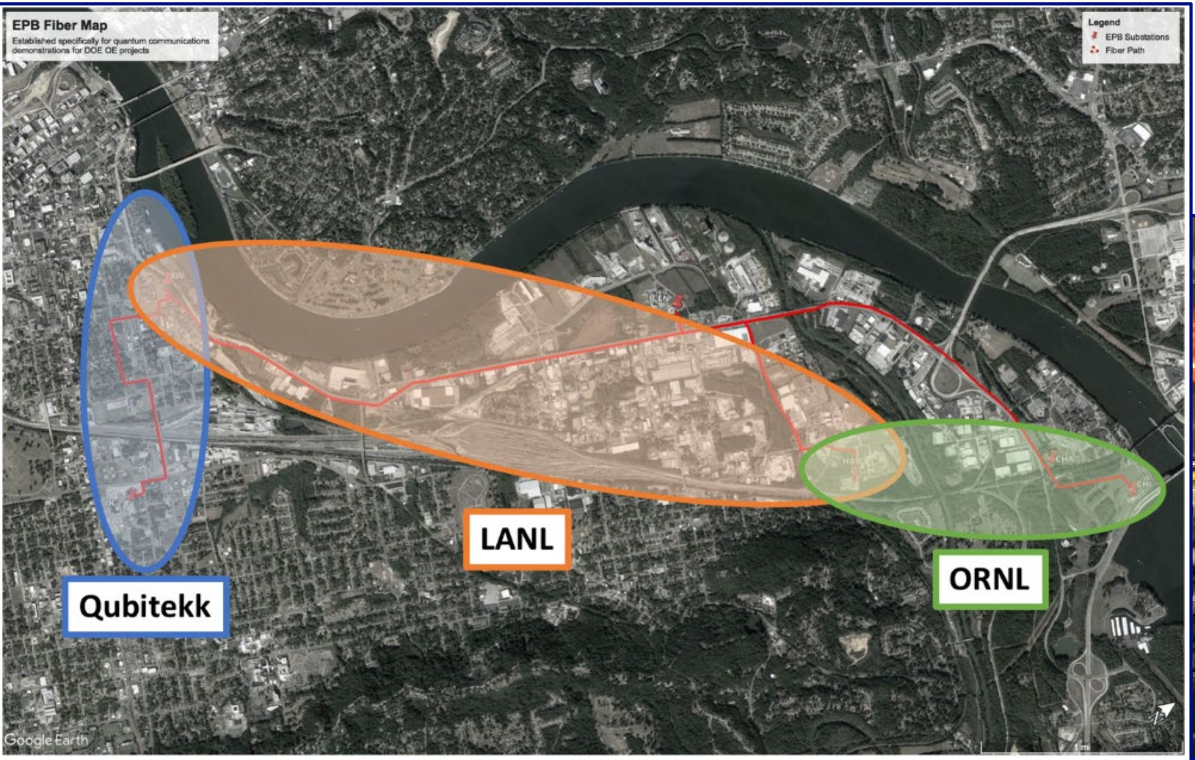


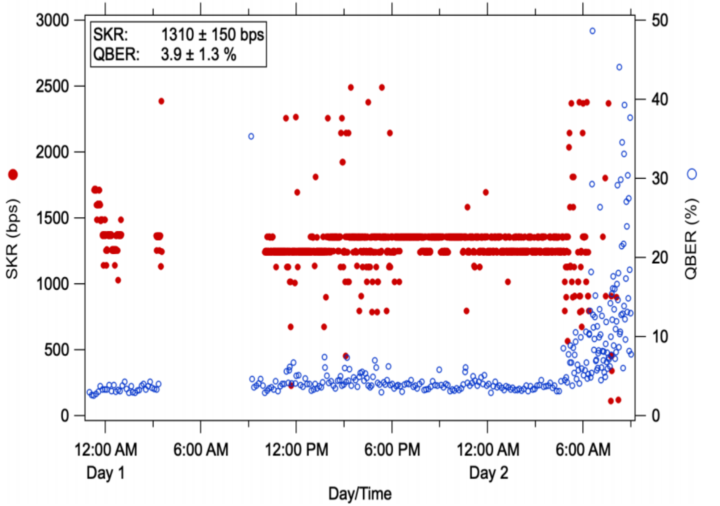
Los Alamos demonstration (2019)





Chattanooga demonstration (2020)





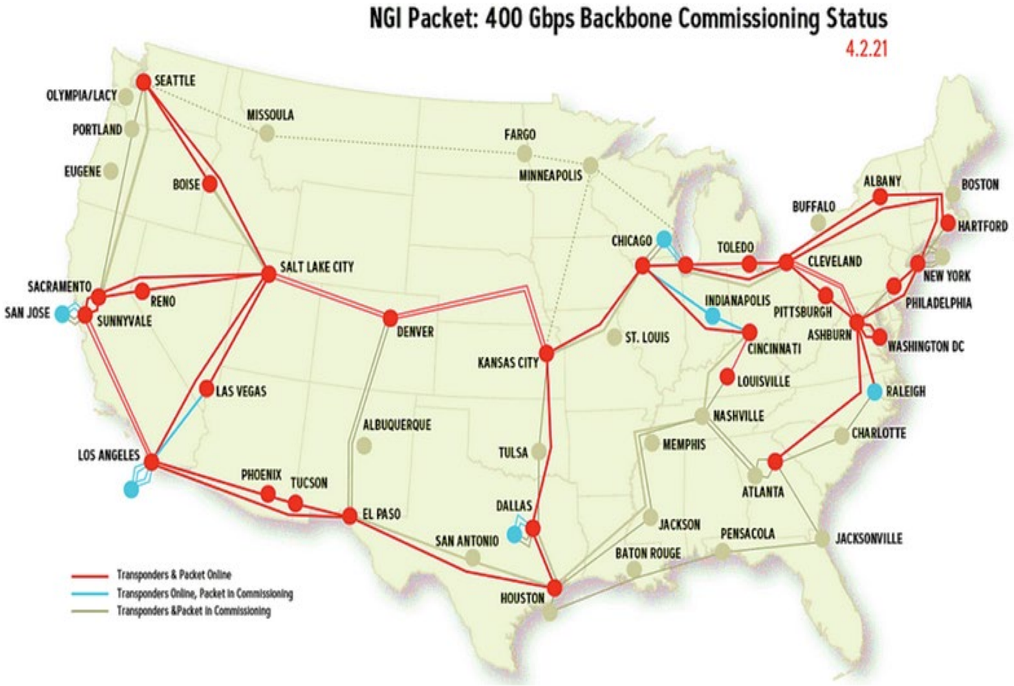
Achievable range depends on detectors

The security of a quantum communication system is contingent on the transmitter sending only one photon at a time (or at most, a few)

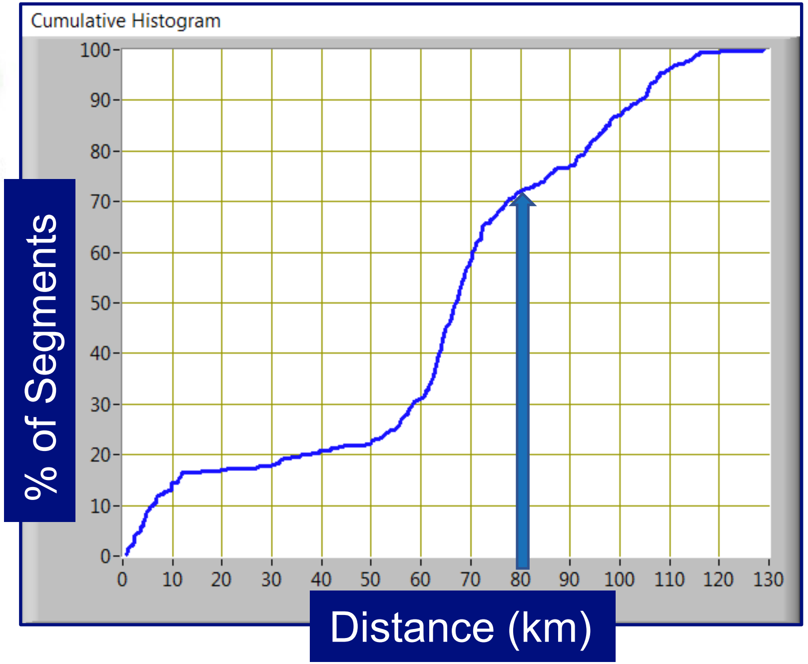
- Maximum transmitted power is fixed (a few femtowatts)
- Loss in the channel is fixed (0.2 decibels/kilometer for fiber)
- Maximum range is determined by the detectors

	Avalanche Photodiode	Superconducting Nanowire	Transition Edge Sensor
Efficiency @ 1550 nm	20%	80%	>95%
Cryogenics?	No	Yes	Yes
Cost per system	$10k	$200k	No commercial product
Achievable range	80 km	150 km	200 km

80 km range would enable 70% of Dept. of Energy's ESnet links



A cumulative histogram of the link lengths shows that 70% of all spans are 80km or less.



Long-Term Vision: Long-Range Networked Quantum Communications

Application layer

Quantum key management layer

Quantum communication protocol layer

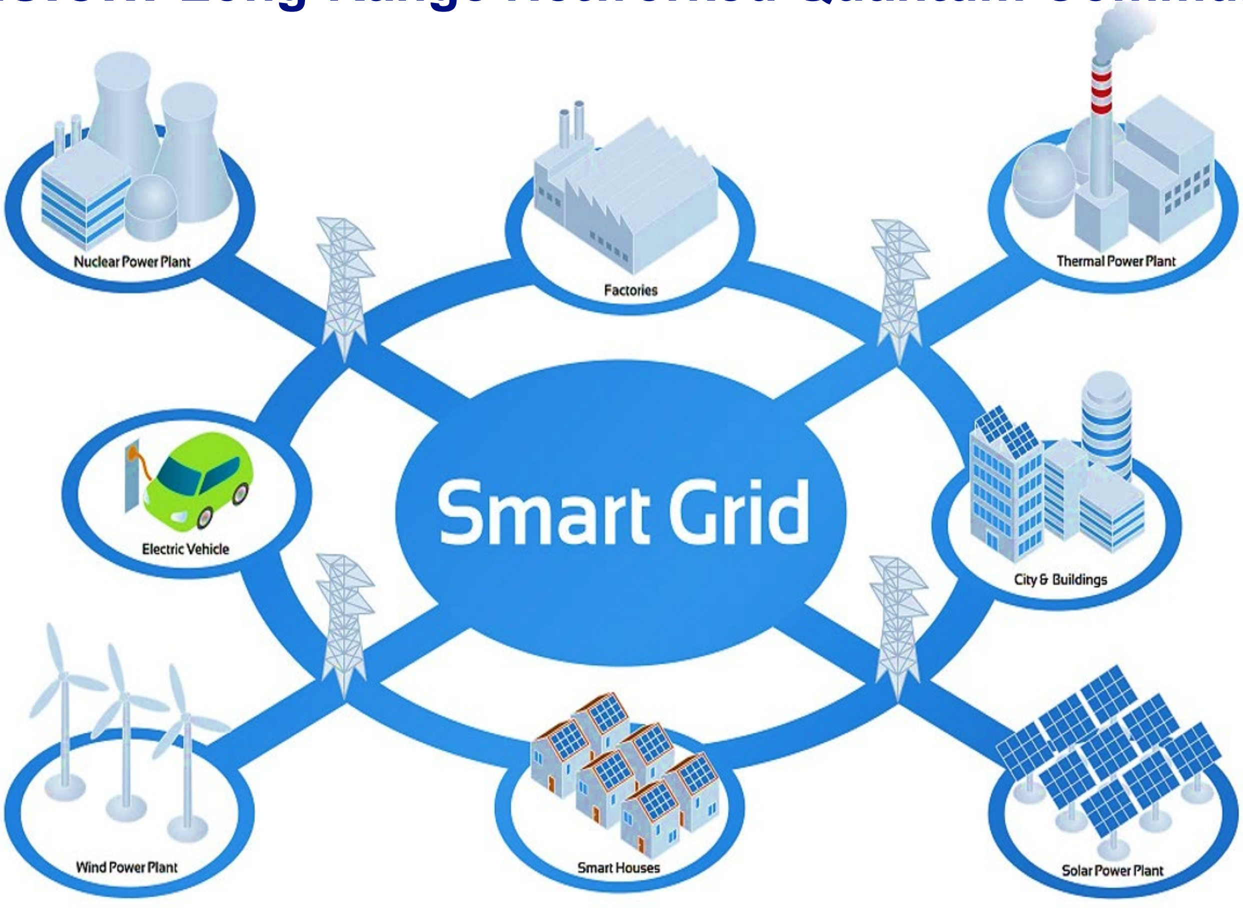


Image courtesy of [SmartGrids.eu.](SmartGrids.eu)

Quantum science provides unparalleled security in many different contexts: especially infrastructure

Quantum Communications

- Quantum signals cannot be copied, split, or examined by an eavesdropper
- Compatible with existing fiber optic infrastructure, especially utilities
- Also compatible with free space communication over line-of-sight

Infrastructure Security

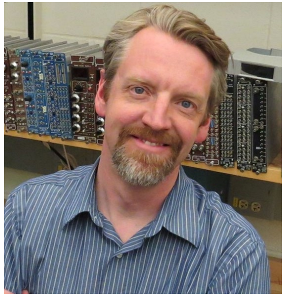
- Trustworthy identification – no spoofing
- Control signals authentic – not manipulated
- Signals encrypted- eavesdroppers just get mush

Cast of Characters

Justin Tripp
CCS-3

Austin Thresher
A-4

Claira Safi
ISR-3

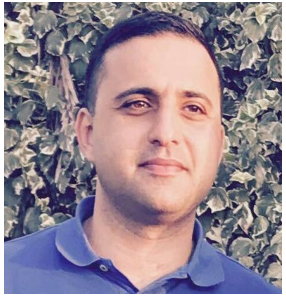


Raymond Newell
MPA-Q

Michael Dixon
A-4

Nathan Lemons
T-5

Nigel Lawrence
A-4



Hassan Hijazi
T-5

Boris Gelfand
A-4

Quantum Computing

Quantum-safe Cryptography

QKDetails

Backup Slides

Difficulties with Today's Public Key Crypto: e.g. RSA

Security lifetime estimates of public keys can erode much faster than predicted

1977: "A new cipher which may take millions of years to break", (M. Gardener, Scientific American)

- Predicted to take 40 quadrillion years to break

1994: Atkins, Graff, Lenstra & Leyland decrypt it in 8 months

- Used 1600 computers on "the internet"

2015: McHugh decrypt in one day

- $30 worth of cloud computing

9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

A ciphertext challenge worth $100

Encrypted text 1977

17 years →

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

Extended Abstract

Derek Atkins[1], Michael Graff[2], Arjen K. Lenstra[3], Paul C. Leyland[4]

[1] 12 Rindge Avenue, Cambridge, MA 02140, U.S.A.
E-mail: warlord@mit.edu
[2] Iowa State University, 215 Durham Center, Ames, IA 50010-2120, U.S.A.
E-mail: explorer@iastate.edu
[3] MRE-2Q334, Bellcore, 445 South Street, Morristown, NJ 07960, U.S.A.
E-mail: lenstra@bellcore.com
[4] Oxford University Computing Services, 13 Banbury Road, Oxford, OX2 6NN, U.K.
E-mail: pcl@ox.ac.uk

Abstract. We describe the computation which resulted in the title of this paper. Furthermore, we give an analysis of the data collected during this computation. From these data, we derive the important observation that in the final stages, the progress of the double large prime variation of the quadratic sieve integer factoring algorithm can more effectively

Decrypted text 1994

Quantum Computing[1] – a (very) brief intro

Regular computers all operate on classical bits, 0 and 1

- Digital electronics make this easy: can duplicate and amplify classical signals

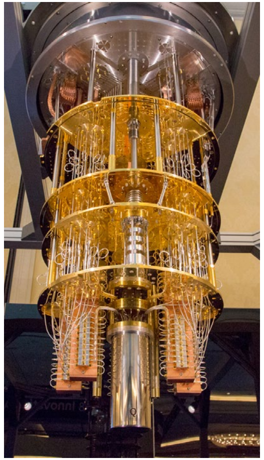
A quantum computer would operate on quantum bits $|0\rangle$ and $|1\rangle$

- Much harder to design: the no-cloning theorem says we can't duplicate signals
- Much harder to build: quantum states are very fragile

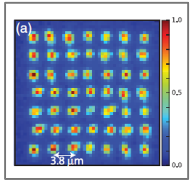
- A classical computer with N bits can be in **any *one*** of the 2^N possible states.
- A quantum computer with N qubits can be in any ***combination*** of the 2^N possible states ***simultaneously***.

- This is a much larger computation space, and can theoretically be used to solve some problems much faster than a classical computer.

- The advantage comes from efficiently discovering group properties of a huge set.



IBM prototype quantum computer



T. Xia et al. (2015)

Array of individual cesium atoms

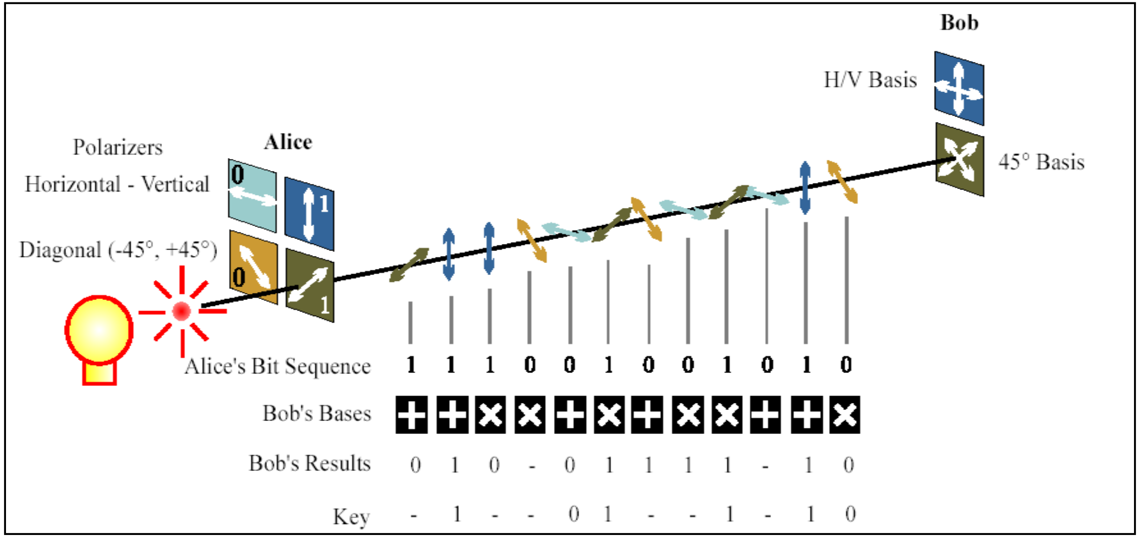
Possible architectures:

- Ions in an electromagnetic trap [2]
- Neutral atoms in an optical trap [3]
- Spin-polarized electrons [4]
- Electrons in a quantum-dot trap [5]
- Nuclear Magnetic Resonance [6]
- Fullerene electron spin resonance [7]
- Nitrogen vacancies in diamond [8]
- Bose-Einstein condensates [9]
- Optical modes in linear optics [10]
- Cavity-photon electrodynamics [11]
- Superconducting Joseph Junctions [12]
- … and more

[1] Benioff (1980) Feynman (1982), Deutsch (1985)
[2] Monroe (1995)
[3] Brennen (1999)
[4] Imamoğlu (1999)
[5] Fedichkin (2000)
[6] Cory (1997)
[7] Komatsu (2005)
[8] Nizovtsev (2005)
[9] Saffman (2017)
[10] Knill (2001)
[11] Miller (2006)
[12] Kaminsky (2004)

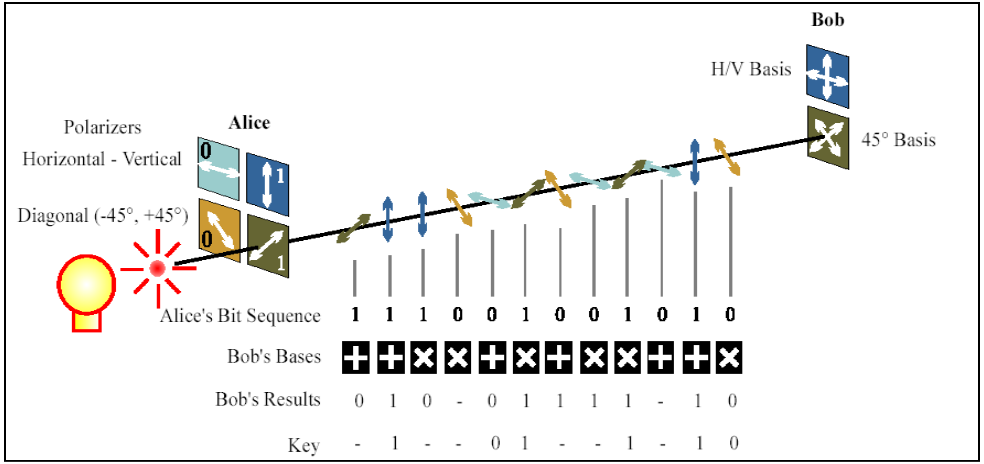
BB-84 Protocol

- Transmitter "Alice" has an attenuated laser and four polarizers
  - **Polarizers are oriented Horizontal, Vertical, Diagonal (+45°), and Anti-diagonal (-45°)**
- Horizontal and Vertical form one basis (HV), Diagonal and Anti-Diagonal another (45°)
- Alice randomly chooses a bit value, 0 or 1, and a basis value, HV or 45°, and sends that photon



BB-84 protocol, continued

- Receiver "Bob" randomly chooses a basis to measure, HV or 45°
- Bob measures bit values in that basis
- Alice and Bob compare basis choices ("sifting")
  - When they used different bases, they discard that bit
  - When they used the same basis, they keep that bit
- Use Forward Error Correction to estimate bit error rate
- Use Privacy Amplification to distill out the truly secret fraction
  - If error rate is too high, secret fraction is zero



Reference

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

International Conference on Computers, Systems & Signal Processing Bangalore, India December 10-12, 1984